REMARKS

The objections and rejections of the claims under 35 USC 112, second paragraph, are attended to above without narrowing and, therefore, without Festo-like limitations even when in response to a statutory requirement, particularly with respect to British English spellings in view of *MPEP* 608.01.

New claim 20 relates to the previously claimed invention by dependence from claim 1 and is supported by page 12, lines 1-17, of the PCT application publication WO 2003/077473.

The rejections of independent claims 1, 10 and 17 under 35 USC 103 for obviousness from the cited Doggett patent and Adam patent publication are traversed, because:

> ... [R]ejections on obviousness cannot be sustained by mere conclusory statements; instead there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness. *Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in KSR International Co. v. Teleflex Inc.*, Fed. Reg. October 10, 2007, 57526, 57528-9.

Merely finding a SIM card in the Doggett and Adam patent and patent publication does not do this. As the patent and publication themselves show, SIM cards have various uses so that one does not necessarily rationally underpin incorporation into another.

In our view, Doggett discloses a method of transferring funds, e.g. in the form of an electronic cheque, from a bank account of a payer to a payee bank account (col. 3, lines 4-5). The method is initiated by a payer, who uses a terminal in the form of computer (work station) which operates in combination with a portable token e.g. a smart card or PCMCIA card which holds the payer's private signature key and a payer certificate associated with the payer's account in a payer bank (col. 8, line 60 to col. 9, line 11 and figure 4 and col. 11, line

48 - col. 12, line 2).

The payer generates an electronic cheque on the computer and appends the payer electronic signature and the payer certificate to the cheque. The payer sends the cheque comprising the electronic payer signature and payer certificate directly to an address of the payee (e.g. by e-mail) (col. 7, lines 49 - 64). The payee has a similar terminal with a token containing a payee private signature key and a payee certificate associated with the payee's bank account in a payee bank (col. 8, line 60 to col. 9, line 11 and figure 4 and col. 11, line 48 - col. 12, line 2).

1. The payee performs first validation of the payer's digital signature by means of the payer's public key, verifies the payer's bank via the payer certificate and performs first examination of the cheque number for recent duplicates (col. 7, line 65 - col. 8, line 4);

2. The payee signs the cheque with the payee signature and payee certificate (col. 8, lines 4 - 11); and

3. The payee sends the modified cheque (i.e. the cheque comprising the payer's electronic signature and certificate and the payee's digital signature and certificate) to the payee bank as identified by the payee certificate (col. 8, lines 15 - 18).

Upon receipt of the cheque, the payee bank performs second validation comprising a validation of both the payer's and payee's signatures by use of the payer's and payee's public keys and checks the payer and payee certificates. The payee's bank credits the sum of money specified in the electronic cheque to the payee's account and clears the electronic cheque with

the payer's bank via check imaging or the like over a financial network (col. 8, lines 19 - 33).

After clearance of the electronic cheque, the payer's bank receives the electronic cheque and performs a third validation comprising a validation of both the payer's and payee's signatures by use of the payer's and payee's public key and checks the payer and payee certificates. If the payer's account comprises sufficient funds to cover the face value of the cheque, then the payer's bank debits the payer's account and electronically sends payment to the payee bank via the financial network (col. 8, lines 34 - 46). If the payer's account does not comprise sufficient funds, then the payer bank returns the electronic cheque to the payee (col. 13, lines 55 - 58).

Thus in summary, Doggett discloses that the following availability of public keys is prerequisite for the disclosed method:

- The payee needs payer's public key, and
- the payer's and the payee's banks need both payer's and payee's public keys.

Further, Doggett discloses that the payee is required to validate the payer's signature and certificate and that both the payer's bank and the payee's bank are required to validate both the payer's and payee's signature and certificate.

Still further, Doggett discloses that the payee's bank credits the payee's account with the sum of money of the electronic cheque BEFORE it has been validated whether the payer's account comprises the necessary funds.

In our view, Adam only discloses a user application that can be stored on a SIM card, thus allowing it to be quickly installed and uninstalled in any cellular phone operating with a SIM card. This is not enough to underpin its combination rationally.

We believe that claim 1 is distinguished by:

> In the central hub, initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initializing a verification of the second signature at the banking institution of the second user and a verification of the first signature at the banking institution of the first user.

Doggett does not disclose this technical feature. On the contrary, it explicitly discloses that the payee bank credits the payee's account with the sum of money of the electronic cheque BEFORE it has been validated whether the payer's account comprises the necessary funds [col.. 8, lines 19 - 33 and col. 8, lines 34 - 46 arid col. 13, lines 55 -58].

Likewise, Adam is silent regarding the abovementioned distinguishing technical feature.

Further, as acknowledged by the examiner, pending claim 1 is distinguished over Doggett by generating signatures in a SIM card.

Therefore, claim 1 solves technical problems not solved by the art:

1) Claim 1 requires exchange of cryptographic keys between the payer and the payer bank and the payee and the payee bank. The combination of Doggett and Adam requires exchange of cryptographic keys between a) the payer and the payer bank in order for the payer bank to validate the payer signature; and b) the payer and the payee bank in order for the payee bank to validate the payer signature; and c) the payee and the payee bank in order for the payee bank to validate the payee signature; and d) the payee and the payer bank in order for the payer bank to validate the payee signature; e) the payer and the payee in order for the payee to validate the payer signature. Thereby, claim 1 solves a first technical problem of reducing the need for cumbersome exchange of cryptographic keys; and

2) Claim 1 solves a second technical problem of preventing a payee from withdrawing the amount of the electronic cheque from the payee account after the payee bank has credited the payee account with the amount of money but BEFORE the payer bank has acknowledged that the payer account contains sufficient funds to cover the face value of the cheque. Claim 1 solves the second technical problem by first initializing a verification of the second signature in the second bank and the first signature in the first bank before initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user. A combination of Doggett with Adam does not solve the second technical problem because, in the combination, funds are credited to the payee account BEFORE the payer account has been checked for containing sufficient funds

Reconsideration and allowance are, therefore, requested.

Respectfully submitted,

William R. Evans
c/o Ladas & Parry LLP
26 West 61st Street
New York, New York 10023
Reg. No. 25858
Tel. No. (212) 708-1930